2. otázka - Informační etika, šifrování

Petr Šťastný

2019-09-22

Contents

1 Hygiena práce s PC

Chceme se vyhnout projevům toho že sedíme dlouhé hodiny a dny u počítače bez pohnutí. Mezi projevy patří bolesti páteře, zad, zápěstí, nebo třeba i očí. Kromě toho že bychom se měli co půl hodiny protáhnout, máme několik základních pravidel pro naši sestavu, abychom tělo co nejméně namáhali.

- Horní část monitoru ve výši očí (i pro laptop)
- Monitor kolem 60-100cm daleko
- Rozmístění programů na monitorech rovnoměrně abychom nestáčeli dlouho hlavu na jednu stranu
- Při sezení, úhel mezi stehnem a lítkem kolem 90 stupňů
- Podložka pro myš nebo kláesnici, případně podobná podložka, abychom měli ruce v jedné rovině
- Sedět vzpřímeně
- Při bolesti zápěstí speciální vybavení jako rozdvojená klávesnice nebo vertikální myš
- Protože sedět v 90 stupňovém úhlu je namáhavé a nikdo to neděla, je dobrá podložka pro nohy s nastavitelným sklonem

2 Informační etika

Aneb jak se správně chovat, a jaké chování očekávat.

Nejčastěji se s tímto pojmem setkáme ve vědeckých prací, v knihovnictví, nebo novinařině, ale náš zajímá spíš etika pro používání a vytváření děl a aplikací.

Základ je nekrást - to se přece nedělá. Nepoužívejte obrázky které nejsou explicitně svobodně licencované, nebo bez souhlasu majitele. A to samé platí třeba i o hudbě.

Naopak ze strany vývojáře, budte fér. Neukládejte a neposílejte si informace, které uživatel nečeká že budou sdíleny. A všechno co sbíráty, pod jakým účelem, a s kým sdílíte, vždycky sepište ve speciálním dokumentu, světově označovaný jako privacy policy.

Ohledně stahování pro vlastní potřebu - v ČR vám nic nehrozí a nikdo vás za to nezavře. Pozor ale na P2P protokoly, jako je třeba Torrent. Pokud používáte torrenty, tak kromě stahování i posíláte soubor - třeba film - ostatním. A to už je proti zákonu a trestně stíhané.

2.1 Licence

Existují licence, kterými můžete definovat jak může být váš obsah využíván. Mezi nejznámější a nejpoužívanější SW lincence pro vaše programy patří:

- MIT - dělej si co chceš, ale neměň licenci a kdo kód napsal.
- GNU GPLv3 - neměň licenci a kdo to napsal, ale musíš zveřejnit zdroják a všechny změny.
- Apache Licence 2.0 - dělej si co chceš, ale musí to mít licenci (ale klidně jinou!) a kdo kód napsal. Programátor má explicitně patentní právo na svůj kód.
- Do What the Fuck You Want to Public Licence - dělej si co chceš.

Pozor - když je kód bez licence, neznamená to, že si můžeme dělat co chceme. Naopak, nic s ním dělat nemůžeme.

Data a média - třeba obrázky - můžeme licencovat pod těmito licencemi:

- CC-BY 2.0 - dělej si co chceš.
- CC0 - všechno mi je jedno, vzdávám se nároku na tohle.
- CC-BY-SA - dělej si co chceš, ale nech tuhle licenci a říkej od koho to máš.

Pro fonty se používá třeba SIL Open Font License, která říká, že si s tím můžu dělat co chci, ale nesmím na tom vydělávat.

3 DRM

DRM je technologie, která nějak zamyká věci, za které jsem zaplatil. Třeba že to nemůžu okládat nebo sdílet - třeba elektronické knihy, hry (Steam), nebo filmy a seriály (Netflix). To se dá obcházet programy, ale toto zbavování se DRM je ilegální. Zajímavost: Illegal Number.

4 Bezpečnost komunikace

Všechno šifrovat! Na webu použít protokol https místo http - výborné je třeba rozšíření https everywhere. Pokud se kdekoliv připojujete přes http, může přijít a vidět všechno co vidíte vy - a kromě toho můžu měnit to co vy vidíte. Jednoduše, naprosto bez problému. Podobný problém mají i protokoly ftp a telnet, které nahrazujte šifrovanými protokoli sftp a ssh.

Používejte adblock a blokátory trackerů - pro prohlížeč můžu doporučit uBlock Origin, nebo pro pokročilé uživatele uMatrix. Obojí je od stejného vývojáře a funguje krásně.

Další důležitá věc je vybrat si prohlížeč. Všechno je v pořádku když si vyberete prohlížeč co běží na Chromiu - třeba Google Chrome, Brave, Operu, Vivaldi, nebo Edge. Když používáte cokoliv od Applu, nemáte na výběr a používáte Safari - dokonce i Firefox je na iOS jenom frontend pro Safari. Nejlepší ale bude použít Firefox. Je to jediný velký prohlížeč, který nemá omezení pro adblocky. Google vydá - nevíme přesně kdy - update, kdy adblocky přestanou fungovat tak jak by měly. Nebudou moct blokovat trackery ani všechny reklamy, naopak pokud neplatíte googlu, adblock bude omezený na nějakých deset tisíc reklam které může umět blokovat - a to je ve skutečném světě směšně nedostatečné. Proč to asi Google udělal - že by proto, že se mu nelíbí že lidi blokují 80 procent jeho výdělku?

Další možnost je blokovat reklamy a trackery už na síťové úrovni - reklama ani nedorazí do vašeho počítače. To umí na Firefoxu - na Chromu ne - rozšíření jako uMatrix, nebo obecně PiHole.

Další základní pravidlo je používat aktualizovaný SW - ať už FOSS nebo placený. Je nebezpečné používat cracknuté programy - alespoň to hoďte do virtuálu!

Citlivé emaily je dobré šifrovat. Pro emailový klient Thunderbird, od Mozilly, je výborné rozšíření Enigma.

Nikdy nenahrávejte na libovolný cloud soubory, u kterých by vám vadilo, kdyby o nich všichni věděli. A když chcete zálohovat, soubory šifrujte. Například programem GPG.

To samé platí o souborech na počítači, kde je ale nejlepší mít rovnou zašifrovaný celý disk - například aplikacemi dm-crypt nebo eCryptfs. To udrží váš harddisk zašifrovaný, když je zrovna počítač vypnutý.

5 Šifrování

Rozlišujeme dva druhy šifrování - symetrickou, která používá symetrický klíč - tedy jeden klíč pro jak rozšifrování tak dešifrování - a asymetrickou, která má pro tyto dvě operace různé klíče.

Použití je asi zřejmé. Zabraňujeme tím tomu, aby někdo věděl co posíláme nebo máme na disku. Taky to můžeme použít k potvrzení toho, že informaci - třeba email - jsme skutečně napsali mi, souhlasíme s tím, a email nebyl od toho podepsání změněn. Toho se využívá například u elektronického podpisu, který nahrazuje běžný podpis například u smluv.

5.1 Symetrické šifrování

U symetrického šifrování je klíč pro jak šifrování tak dešifrování totožný. Tedy zadáme heslo kterým rozšifrujeme data, a stejným heslem to i zašifrujeme. Například správce hesel to používá pro zašifrování hesel uložených na počítači. Když ho nastartujete a zadáte heslo tak hesla odšifruje, a před ukončením aplikace je zase zašifruje.

Taky šifrování disku funguje na tomto principu. Stejně jako fungovala třeba enigma. Jedna konfigurace zprávy jak šifrovala tak dešifrovala.

A ještě jednu poznámku ohledně bezpečnosti: nejlepší heslo je to, co si člověk snadno zapamatuje, ale počítač ho těžko uhodne. Tedy hodně dlouhé. Může to být třeba nějaký citát, třeba váš vlastní. Nebo část básničky. To je jedno, hlavně aby si to šlo dobře zapamtaovat. Většina mých hesel - těch které mám v hlavě, a ne ve správci hesel - mají přes 60 znaků, většina - třeba heslo do banky - má přes 100 znaků. A snadno jsem si to zapamatoval, jsou to dvě věty.

5.2 Asymetrické šifrování

Asymetrické šiforávní funguje tak, že máme jeden klíč - veřejný - kterým informace šifrujeme, a druhý - privátní, soukromý - kterým informace můžeme dešifrovat.

Tedy když nám třeba chce někdo poslat zašifrovanou zprávu, třeba email, tak mu prostě dáme veřejný klíč. Ten může být často i dostupný na internetu, na tzv keyserverech. Můj klíč je nahraný tradičně na třech keyserverech, takže když mi někdo chce poslat zašifrovaně zprávu, prostě zapne GPG - program na šifrování - a zvolí možnost importu klíče podle mé emailové adresy. Klíč se mu stáhne a může začít šifrovat.

Jakmile tato zpráva dorazí, použijeme soukromý klíč abychom ji dešiforvali. Díky tomu funguje to, že všichni nám mohou poslat bezpečnou zašifrovanou zprávu, ale nikdo kromě nás nji nerozšifruje.

S tím souvisí elektronický podpis. Ten funguje tak, že místo šifrování vezmeme soukromý klíč a pomocí něj zašifrujeme hash dokumentu. Kdokoliv má náš veřejný klíč může hash dešifrovat z kontrolovat. Podpis je tedy platný pouze pokud se soubor od našeho podepsání nezměnil. Já třeba takhle podpisuji emailové zprávy, takže si všichni můžete ověřit, že email opravdu přišel ode mě a nikdo si s ním nehrál.

5.3 Web of trust

S tím souvisí Web of Trust. Pokud vám přijde email s mým veřejným klíčem - jak víte že ten veřejný klíč je můj? Třeba je ten klíč útočníka, který se za mě vydává. K tomu máme Web of Trust. Myšlenka je v tom, že Luboš má nový veřejný klíč. Tak mi ho pošle, a osobně mi řekne že tenhle klíč je jeho. Já mu třeba i zkontroluju občanku, a jeho veřejný klíč podepíšu - oznamuji takhle světu, že Lubošovi věřím. Takhle to dělat se všemi se kterými chci komunikovat je nepraktické. Takže k tomu abych někomu důveřoval mi stačí to, že mu důvěřuje Luboš.

6 Zdroje

- Ergonomie a hygiena používání PC: interní wiki Alza.cz
- Informační etika: wikisofia.cz/wiki/Informační_etika
- Wen: Information ethics
- Lincence: ChooseALicense.com
- Wen: Digital rights management
- GPG manpage
- Wcz: Kyberšikana
- Wen: Web of Trust
- Wen: Public key encryption